United States Army
Criminal Investigation Command

Media contact:
703-806-0372

For Immediate Release

CID Cyber Lookout
On Point for the Army

Warning to Online Holiday Shoppers
CID Offers Tips for Army Community to Avoid Swindlers During Height of 'Rip-Off" Season

FORT BELVOIR, Virginia, December 3, 2008 – The U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) has teamed up with the Federal Trade Commission (FTC) to help Soldiers, family members and Army civilians stay safe while shopping online this holiday season.

As increasing number of consumers do the majority of their holiday shopping online and swindlers have taken notice and devised a wide range of schemes to capitalize on the relative anonymity of cyber space. The CCIU and FTC offer the following tips to help thwart these online crooks:

Check out the seller: If you have not used a particular online shopping site, do some independent research. Call their phone number to verify that you can reach them if issues come up with your purchase. If they don't have a phone number, you should take your business elsewhere. Also, search the Internet to see if anyone else has had a positive or negative experience with the shopping site.

Read return policies: Make sure the online shopping site has policies that meet your needs and expectations. Some sites charge shipping and handling for returns, as well as a restocking fee. Sites with unclear or questionable policies should be avoided.

Know what you're getting: Read the product description closely. If name-brand items are sold at an extremely low price, they could be counterfeit or stolen. Remember the old adage: "If it's too good to be true, it probably is."

Don't fall for a false e-mail or pop-up: Legitimate companies do not send unsolicited e-mail messages asking for your password, login name, or financial information, but scammers do. Delete these e-mails without clicking on any links, since doing so could install spyware or other malicious programs on your computer.

-more -

Look for signs a site is safe: When you are ready to buy something from a seller you trust, look for signs that the site uses a secure connection - such as a closed padlock on the browser's status bar - before you enter your personal and financial information. When you are asked to provide payment information, the beginning of the Web site's URL address should change from http to shttp or https, indicating that the purchase is encrypted or secured.

Secure your home computer: At a minimum, your computer should have anti-virus and anti-spyware software and a firewall. Security software must be updated regularly to help protect against the latest threats. Set your security software and operating system to update automatically.

Consider how you'll pay: Credit cards generally are a safe option because they allow buyers to seek a credit from the issuer if the product is not delivered or is not what was ordered. Also, if your credit card number is stolen, you usually will not be liable for more than $50 in charges. Do not send cash or use a money-wiring service because you will have no recourse if something goes wrong.

Keep a paper trail: Print and save records of your online transactions, including the product description and price, the online receipt, and copies of any e-mail you exchange with the seller. Read your credit card statements as soon as you get them to make sure there are no unauthorized charges.

If a member of the Army family believes they have fallen victim to an online shopping scam, CID advises to notify the appropriate law enforcement agency as soon as possible. For crimes occurring on an Army installation, contact the local CID office. For crimes occurring elsewhere, contact the Internet Crime Complaint Center (IC3) online at http://www.ic3.gov. IC3 is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center and serves as a clearinghouse for Internet crime complaints.

To learn more about online safety, visit the FTC's OnGuard Online site at http://onguardonline.gov

To learn more about the CCIU and CID Cyber Lookout, visit http://www.cid.army.mil/CCIU.html

# # #

CID Lookout is a U.S. Army Criminal Investigation Command (USACIDC) initiative to partner with the Army community by providing a conduit for members of the Army family, to help prevent, reduce and report felony-level crime.